



Regione Umbria - Assemblea legislativa

“Leggere e raccontare il Cybercrime: fonti ufficiali, dati e deontologia”

7 Ottobre 2026

In sintesi

Si è svolto ieri a Palazzo Cesaroni a Perugia un incontro sulla cybersicurezza in cui è stato presentato il “Manifesto per l’informazione e la comunicazione responsabile degli incidenti di Cybersicurezza”, nato dalla collaborazione tra Ordine regionale dei Giornalisti dell’Umbria e Regione Umbria. Intervenuti, fra gli altri, la presidente dell’Assemblea legislativa Sarah Bistocchi e il vicepresidente della Regione Umbria, Tommaso Bori

(Acs) Perugia, 7 ottobre 2026 - Nella sala Brugnoli di Palazzo Cesaroni si è svolto ieri pomeriggio un incontro sulla cybersicurezza in cui è stato presentato il “Manifesto per l’informazione e la comunicazione responsabile degli incidenti di Cybersicurezza”, frutto di un protocollo d’intesa nato dalla collaborazione tra Ordine regionale dei Giornalisti dell’Umbria e Regione Umbria, realizzata in collaborazione con CSIRT Umbria (Computer Security Incident Response Team).

Il “Manifesto per l’informazione e la comunicazione responsabile degli incidenti di Cybersicurezza” ha l’intento di fornire a chi fa informazione un quadro di riferimento condiviso per raccontare gli incidenti cyber in modo che il diritto di cronaca e il diritto della cittadinanza a essere informata non si traducano, involontariamente, in un danno aggiuntivo per le vittime, per le indagini in corso o per la sicurezza collettiva. Consta di 15 principi per la corretta comunicazione, rivolti sia ai giornalisti che agli Uffici stampa e Comunicazione degli enti: “Verificare prima di pubblicare, sempre; aggiornare e correggere quando emergono nuovi elementi; proteggere le vittime; non fare da cassa di risonanza agli attaccanti; non pubblicare dettagli tecnici che facilitano nuovi attacchi; usare un linguaggio corretto, non sensazionalistico; contestualizzare l’impatto reale, senza esagerare né minimizzare; dare voce a chi è stato colpito con tempi ragionevoli; sostenere la cultura della prevenzione di Cybersicurezza; evitare di fornire elementi che possano ostacolare le indagini; verificare tutto ciò che è stato prodotto dall’IA; stabilire un flusso e un piano della comunicazione dell’incidente; preparare alcuni messaggi iniziali per dare informazioni in caso di attacco cyber; individuare canali alternativi di comunicazione; programmare simulazioni pratiche per verificare che il piano di gestione della crisi cyber sia realmente efficace”.

Dopo i saluti istituzionali della presidente dell’Assemblea legislativa, Sarah Bistocchi, del vicepresidente della Regione Umbria, Tommaso Bori, del presidente dell’Ordine regionale dei Giornalisti dell’Umbria, Luca Benedetti e della presidente del Corecom umbro, Michela Angeletti, i lavori si sono concentrati sugli ultimi dati riguardanti gli attacchi informatici, illustrati dalla presidente della Clusit (Associazione italiana per la sicurezza informatica) Anna Vaccarelli, quindi sui report e sulle funzioni di Cert-AgID, struttura dell’Agenzia per l’Italia Digitale che ha la funzione istituzionale di mantenere e sviluppare servizi di sicurezza preventivi e funzioni di accompagnamento utili per la crescita e la diffusione della cultura della sicurezza informatica, presentati dal responsabile Gianni Amato. Interventi anche della Polizia Postale di Perugia, con il vicequestore aggiunto e dirigente del Cosc (Centro operativo per la sicurezza cibernetica) Francesco Verducci, quindi di Marco Mencacci, dirigente Infrastrutture digitali e cybersicurezza della Regione Umbria, che ha presentato le iniziative nell’ambito della sicurezza informatica intraprese dalla Regione Umbria e dell’Ordine dei giornalisti. Ha moderato l’incontro Mirko Loche, consigliere dell’Ordine dei giornalisti dell’Umbria.

“Quello di oggi - ha detto la presidente Bistocchi - è un primo appuntamento dopo la firma del protocollo tra Regione, Csirt Umbria e Ordine dei giornalisti proprio sulla cybersicurezza e l’informazione, per avviare e rafforzare una collaborazione su sicurezza informativa, prevenzione e comunicazione pubblica. ‘Leggere e raccontare il cybercrime’ significa confrontarsi con una delle sfide più complesse del nostro tempo. Una sfida che non riguarda soltanto la sicurezza informatica, la tecnologia o le forze dell’ordine, ma investe la qualità della nostra democrazia, la consapevolezza dei cittadini e, in maniera particolare, il ruolo dell’informazione. Perché di fronte al cybercrime il primo strumento di difesa, prima ancora della tecnologia, è la conoscenza. E la conoscenza passa anche attraverso un’informazione corretta, verificata, responsabile. Il crimine informatico ha caratteristiche che lo rendono particolarmente insidioso. È veloce, spesso invisibile, attraversa i confini nazionali e può colpire contemporaneamente persone, imprese, istituzioni e infrastrutture. Può assumere forme diverse: dalla sottrazione di dati personali alle frodi online, dagli attacchi alle infrastrutture digitali alle campagne di disinformazione, fino alle forme più sofisticate di manipolazione e di ricatto. Ma c’è un elemento che accomuna fenomeni così diversi: la vulnerabilità delle persone. Dietro un dato rubato, un’identità violata, un conto svuotato o un’organizzazione colpita da un attacco informatico ci sono persone, famiglie, lavoratori, imprese e comunità. In merito all’incontro di oggi, ci sono tre parole che considero centrali: fonti ufficiali, dati e deontologia. Sono tre elementi strettamente connessi. Le fonti ufficiali sono indispensabili per comprendere la dimensione reale del fenomeno. I dati ci aiutano a superare impressioni e allarmismi e a costruire una rappresentazione fondata sulla realtà. La deontologia ci ricorda, infine, che non tutto ciò che può essere pubblicato deve necessariamente essere pubblicato nello stesso modo, con gli stessi toni e senza una valutazione delle conseguenze. Il cybercrime non è soltanto una questione di sicurezza. È anche una questione democratica. La nostra democrazia si fonda sulla possibilità dei cittadini di essere informati e di formarsi liberamente un’opinione. Se le informazioni vengono manipolate, se le fonti non vengono verificate, se la disinformazione viene diffusa più rapidamente delle notizie corrette, il problema non riguarda più soltanto il mondo digitale. Riguarda la nostra capacità collettiva di distinguere il vero dal falso e, quindi, di partecipare consapevolmente alla vita democratica. Per questo le istituzioni hanno una responsabilità importante, quella di investire nella formazione, nella prevenzione, nella cultura della sicurezza digitale e nella capacità dei cittadini di riconoscere i rischi. E nessuna strategia di prevenzione può prescindere dall’informazione”. PG

Source URL: *<http://consiglio.regione.umbria.it/informazione/notizie/comunicati/leggere-e-raccontare-il-cybercrime-fonti-ufficiali-dati-e>*

List of links present in page

- <http://consiglio.regione.umbria.it/informazione/notizie/comunicati/leggere-e-raccontare-il-cybercrime-fonti-ufficiali-dati-e>